# Machine Learning-Based Framework for Detecting and Mitigating DoS Attacks in Mobile Ad-Hoc Networks (MANETs)

DR BABANGIDA ZUBAIRU, AISHA IBRAHIM GIDE
Department of Computer Science
Umaru Musa Yar'adua University
Katsina, NIGERIA

Abstract: - A Mobile Ad-hoc Network (MANET) is a dispersed, decentralized network of mobile wireless nodes that interacts directly with one another without the use of centralized management or stationary base stations. In a MANET's, nodes are always moving, randomly and unpredictably, which presents a number of difficulties and leaves these networks especially open to different security risks. These infrastructure-less networks are especially vulnerable to security threats like Denial of Service (DoS) attacks, black hole attacks, network partitioning, and node selfishness since they lack central management and have limited hardware resources. This paper presents a framework for detecting and mitigating Denial of Service (DoS) attacks in Mobile Ad-hoc Networks (MANETs) using various machine learning models, including Support Vector Machine (SVM), Random Forest, Neural Network, and K-Nearest Neighbors (KNN). In order to simulator both normal and attack traffic, the proposed system generate synthetic datasets from simulation, trains these models, and assesses their efficacy using a number of performance metrics, such as accuracy, scalability, energy consumption, resource utilization, and network throughput. The results shows that Random Forest, SVM, KNN, and Neural Networks have the highest detection accuracy. Neural Networks also showed better network performance and scalability, which made them appropriate for high-traffic situations. On the other hand, KNN is observed to have less energy consumption, which made it an effective choice for situations where resources are limited.

Key-Words: DoS Attack Detection, Mobile Ad-hoc Networks (MANETs), Machine Learning Models, Neural Network

Received: May 14, 2024. Revised: January 26, 2025. Accepted: March 27, 2025. Published: June 2, 2025.

## 1. Introduction

A Mobile Ad-hoc Network (MANET) is a network made up of mobile nodes connected using wireless multi-hop technology. By enabling each node function as a router independently, network functionality can be attained without the need for a fixed infrastructure [1] MANET is rapidly gaining traction and is composed of affordable, compact, and reliable equipment. Adaptive and self-organizing, devices can easily add or remove nodes from these networks while maintaining connections. Search and rescue operations, military operations, and sensor networks are just a few of the scenarios in which MANETs can be applied [2]. MANETs' rapid deployment and dynamic configurability are two important characteristics that have added to their growing popularity. MANETs can provide essential internet access in the event of a disaster if there is a chance that the current communication infrastructures would be destroyed. However, the routing algorithm in charge of enabling packet exchanges between a MANET's migrating nodes becomes more crucial in dictating the network's performance in terms of throughput and end-to-end latency. MANETs are characterized by a dynamic topology in which nodes move around a lot, which affects network security [3]. MANET topologies are inherently unstable, undergoing frequent and random changes over time. Managing connections and routing communications becomes extremely difficult in the absence of centralized control or infrastructure [4]. The network's dynamic structure, which includes nodes changing locations frequently, makes it particularly susceptible to attacks like flooding, in which an overwhelming volume of data is purposefully generated to reduce performance. Because of the dynamic topology and lack of central authority, attacks are more dangerous, making it more difficult to ensure secure and effective communication [5]. Securing MANETs is a significant challenge to research, despite the fact that they are vulnerable to a range of attacks that compromise network security. A significant risk that must not be disregarded is the Denial of Service (DoS) attack. In DoS attack, an attacker floods the network with hundreds or thousands of useless packets, flooding the victim's machine. The network's capacity and performance may be severely reduced by this enormous traffic, making it unable to carry out its operations and offer services to valid nodes [6]. The main objective of this paper is to experiment the application of machine learning models to in mitigating DoS attack in MANET. To achieve this first we implement MANET network and DoS attack in the network, then we added detection and mitigation algorithms designed especially for MANETs and machine learning

models like Support Vector Machine (SVM), Random Forest, Neural Network, and Kth Nearest Neighbor (KNN) on generated datasets that simulate both normal and attack traffic. Once trained, the best-performing model is used to predict and visualize traffic patterns in a simulated MANET environment, assisting in identifying attack nodes. To enhance network security, the framework also simulates critical performance measures, such as energy consumption and throughput, to evaluate the impact of attacks and the effectiveness of the detection models. Improved detection performance and resilience against possible DoS attacks in MANETs are ensured by this integrated technique. The remainder of the article is structured accordingly. Section 2 provide an overview of the research background. Section 3 discusses the literature review. Section 4 introduces the proposed methodology and the framework for DoS attack mitigation in Manet. We provide the experimental design, data collection and preprocessing, implementation of the machine learning model and the performance metrics used for evaluations Section 5. Section 6 contains the results and analysis. We discuss our research, implication of the findings and future directions in Section 7. Section 8 concludes the paper.

## 2. Overview of manets

The 1970s saw the introduction of packet-switched communication, which allowed wireless networks to be developed independently of wired infrastructure. Wireless networks become widely used as a result of this technology's mobility and flexibility. The telecoms industry has changed significantly in the last several decades. Rapid advancements in wireless technology have made life much better and made it possible to access network connections practically constantly from anyplace. The majority of people increasingly rely on mobile devices for their everyday activities since these technologies have grown more widely available and more affordable [7].

Autonomous mobile nodes that dynamically establish multi-hop communication networks are the building blocks of a Mobile Ad Hoc Network (MANET). But these networks are open to all kinds of attacks, such as selfish conduct and denial of service (DoS) attacks. Because the broadcast mechanism is resource-intensive and mobile nodes have limited resources, MANETs are especially vulnerable to denial of service (DoS) attacks. One major problem in MANETs is ensuring secure communication. Due to its distinct features, which include dynamically changing topology, unreliable wireless connectivity, a lack of centralized monitoring, and the absence of a certification authority, traditional security techniques intended for structured networks sometimes do not apply to MANETs [8]. In MANETs, the absence of dedicated routers means that routing is handled entirely by the peer nodes that make up the network. When designing routing protocols for MANETs, enhancing throughput and minimizing packet loss are key considerations. These protocols are generally classified into three main categories, as illustrated in Figure 1.

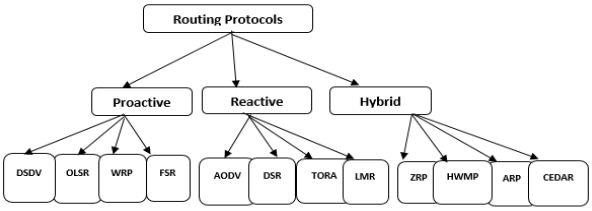


Fig. 1. Routing Protocols in MANETs

Proactive routing protocols, such as Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR), Wireless Routing Protocol (WRP), and Fisheye State Routing (FSR), are also referred to as table-driven protocols. Every node on the network registers routes to every other node through proactive routing protocols, which keep track of every route even when they are not needed. These protocols maintain up-to-date routes for every node in the network by routinely exchanging control information between nodes. They also respond to the appearance of a new node or the removal of an existing node from the network topology. The two most well-known proactive protocols are Optimized Link State Routing (OLSR) (Zhiyuan & Jinhong, 2010) and Destination-Sequence Distance-Vector (DSDV) (Mahdipour, Rahmani, & Aminian, 2009). Proactive routing aims to precompute all feasible paths by periodically distributing information throughout the network. Updates are propagated to maintain routing tables up to date whenever a change happens. As a result, in emergency and rescue situations, it is crucial to continuously evaluate the paths connecting nodes in order to gradually evacuate those affected [9]. However, these protocols can be inefficient in their use of bandwidth, and the overhead can become significant as the network is frequently flooded with updates to maintain accurate routing tables [10].

Reactive routing protocols, also known as on-demand protocols, initiate the route discovery process only when a communication between a source and a target node is required. With this method, the overhead usually related to proactive routing where routes are maintained up to date is minimized. Reactive routing creates a communication channel between the source and

target nodes by having the source node bombard the network with Route Request (RREQ) packets, to which intermediary nodes reply with Route Reply (RREP) packets. Data transmission begins as soon as the path is created. Reactive protocols provide the primary advantage of having nodes that only retain data on active routes; network-wide data is not maintained. Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Temporally Ordered Routing Architecture (TORA) are significant examples of reactive routing systems [11].

Hybrid routing protocols: In order to overcome the limitations of each strategy, hybrid routing protocols integrate both the advantages of proactive and reactive approaches. They use reactive methods for communication outside of these zones and retain proactive channels within the network's concentrated sections. This hybrid strategy creates a compromise between low overhead and effective bandwidth use and immediate availability of routes. Hybrid Wireless Mesh Protocol (HWMP), which combines proactive and reactive techniques to optimize routing in wireless mesh networks, and Zone Routing Protocol (ZRP), which uses proactive routing within a defined zone and reactive routing for communication between zones, are two examples of hybrid protocols. Other examples include CEDAR (Core-Extraction Distributed Ad Hoc Routing) and Adaptive Routing Protocol (ARP), which combine proactive and reactive techniques to improve routing effectiveness and adaptability in dynamic [12].

### 2.1 Denial of Service (DoS) attack in Manets

A Denial of Service (DoS) attack occurs when a single machine sends an overwhelming amount of packets to a server, overloading its bandwidth and resources. By creating a one-to-one attack vector that makes mitigation and prevention attempts more difficult, this kind of active attack is a potent technique for interfering with internet services. A DoS attack often targets the server's capacity to process valid requests and causes service disruptions by employing one machine to create a large volume of traffic [8]. Attacks known as denial of service (DoS) have the potential to seriously affect the availability and performance of mobile ad hoc networks (MANETs). The following are some typical DoS attack kinds that target MANETs:

Jamming Attack: In this technique, an attacker uses radio signals to obstruct or interfere with the channels that network nodes use for communication. The attacker prevents authorized nodes from sending or receiving data by interfering with wireless connectivity.

Flooding Attack: The attacker floods the network with too many routing requests or traffic, which overloads it and uses up all of its resources. Increased latency, decreased throughput, and even network collapse may result from this.

Depletion Attack: This attack makes mobile nodes complete pointless tasks or use excessive amounts of energy in an attempt to deplete their energy reserves. To exhaust the battery life of the targeted nodes, an attacker can, for example, send large quantities of control packets or repeatedly start route finding procedures.

Black Hole Attack: In this type of attack, a malicious node falsely advertises itself as having a valid route to the destination. Once other nodes send data packets to this node, it either drops the packets or forwards them incorrectly, leading to packet loss and communication failures.

Sybil Attack: The attacker creates multiple fake identities or nodes within the network. By introducing these bogus nodes, the attacker can manipulate routing decisions, disrupt network operations, or overwhelm network resources. These DoS attacks exploit the unique characteristics of MANETs, such as their dynamic topology and lack of centralized control, making them challenging to detect and mitigate.

### 2.2 Importance of Dos Attacks Mitigation in Manets

In a mobile area network (MANNET), mobile nodes function autonomously and can effortlessly create direct communication channels with one another. They can move freely in different directions and at varied speeds inside the infrastructure-less network. The way the ad hoc network functions are distinct, and node cooperation is essential to transmitting communication data from the primary data sources to the mobile nodes that are meant to receive it. These nodes have no restrictions on their movement and are completely battery-powered. Mobile nodes are free to join or exit the dynamic network whenever they choose, and they are not dependent on a single, centralized authority to make choices. This core characteristic of not requiring a fixed infrastructure is essential for enabling communication [13]. However, these same characteristics also leave MANETs open to several kinds of attacks, most notably Denial of Service (DoS) attacks. Attackers might severely reduce the performance and dependability of the network by taking advantage of these flaws to undermine communication, exhaust node resources, or alter network routing. Sensitive data could be compromised in addition to causing communication disruptions in the event of a successful DoS attack. In Mobile Ad Hoc Networks (MANETs), preventing

denial-of-service (DoS) attacks is crucial to preserving network performance and stability. Due to their dynamic and decentralized structure, MANETs are especially susceptible to these kinds of attacks, which can flood the network with excessive and meaningless traffic. Flooding causes higher latency, lower throughput, and more packet loss, all of which lower the standard of network services. Effective mitigation strategies help ensure that the network can handle normal traffic loads efficiently, preserving its overall functionality and preventing performance degradation. Moreover, protecting sensitive data and ensuring service availability are critical aspects of DoS attack mitigation in MANETs [14]. These networks are frequently utilized in high-stakes situations when data integrity and anonymity are crucial, such as military operations, emergency communications, and disaster response. The network can defend against such attacks, keep up service, and preserve the integrity and confidentiality of the sent data by putting strong mitigation measures in place. Different research groups are creating methods for preventing attacks using DoS.

## 3. Literature review

The authors of [14], examine a number of aspects of Distributed Denial of Service (DDoS) assaults in Mobile Ad-hoc Networks (MANETs) and offer countermeasures to these threats. DDoS attacks, according to them, are dangerous threats that cause a major decline in network performance by continuously flooding the network with fake packets. In order to simulate ad hoc routing protocols and evaluate network performance, the study emphasizes the usefulness of Network Simulator (NS3). Additionally, it looks at detection mechanisms like threshold timestamps and node response times to spot malicious activity. The literature emphasizes how difficult it is to identify and mitigate DDoS attacks and how simulation tools and machine learning can help improve network security. More practical, flexible, and effective solutions are needed to mitigate DDoS attacks in MANETs, especially when it comes to fixing non-legitimate nodes' vulnerabilities, enhancing detection mechanisms, and incorporating cutting-edge technologies like machine learning into already-existing frameworks. Furthermore, by examining node behavior and energy usage, writers in [15] have investigated the application of machine learning techniques, such as Feed Forward Back Propagation Neural Networks (FFBPNN), to improve attack detection. The authors identified and eliminated the malicious nodes from the route by comparing the energy consumption and delay metrics of the nodes to those of suspected malicious nodes. Additionally, the authors of [3] evaluated how three routing protocols in Mobile Ad Hoc Networks (MANETs) Zone Routing Protocol (ZRP), Ad hoc On-Demand Distance Vector (AODV), and Location-Aided Routing (LAR) were affected by Distributed Denial of Service (DDoS) attacks. It was discovered that DDoS attacks severely reduced network performance using the DDoS Attack Simulation Model (DDoSM) with Network Simulator 2 (NS-2). The throughput of AODVs decreased by 67.3%, LARs by 62.8%, and ZRPs by as much as 57.1%. Additionally, AODV saw the most rise in end-to-end delay (98.71%), with increases in LAR and ZRP coming in second and third, respectively, at 97.1% and 96%. Attacks had an effect proportionate to the number of perpetrators, with more than ten attackers having the ability to bring down the network. The study identified a need for comparative analysis of these protocols under different types of attacks, such as blackhole and greyhole attacks, and for the exploration of adaptive mechanisms to enhance protocol resilience. To address several attack vectors in MANETs, future research should concentrate on creating hybrid protocols with integrated security measures. Moreover, an Intrusion Detection System (IDS) designed to identify DoS attacks in MANETs was proposed by [16]. Support Vector Machines (SVMs) are the classification technique used by this intrusion detection system (IDS) to detect and stop DoS attacks. According to experimental findings, the intrusion detection system (IDS) efficiently identifies and neutralizes denial-of-service (DoS) assaults with a high detection rate and limited processing time. The detection rate was also found to be constant, irrespective of node mobility or network size. In addition, the authors in the study [17] presented a novel approach to protect networks against DoS attacks called "monitoring detection and rehabilitation." This method measures actual values to assess the reliability of sensor nodes. By obtaining a 20.87% increase in Packet Delivery Ratio (PDR), the suggested solution outperformed the current "trust enhanced anonymous-on-demand routing protocol." Using blockchain technology, Cochain-SC is a decentralized and secure DDoS collaboration framework that was introduced in 2019 [18] for DDoS mitigation. By incorporating Ethereum's smart contract technology, the authors enhanced cooperation amongst Software-Defined Networking (SDN) domains. DDoS mitigation on both the intradomain and interdomain levels was supported by this blockchain-based method. They measured the unpredictability of the data using sFlow and the Intra Entropy-based Scheme (I-ES). Network traffic irregularities were automatically recognized by the I-

ES inside each domain. Additionally, the Intra-Domain Mitigation (I-DM) mechanism was used to mitigate illegal traffic within the SDN domain. The suggested model's cost-effectiveness, flexibility, efficiency, and security were evaluated in order to determine its efficacy. The authors of [19] evaluate sequence numbers to a threshold value that is dynamically generated using timers in order to find black hole nodes. Additionally, they alert nearby nodes to the rogue node. Nevertheless, this method entails the computational expense of determining dynamic threshold values and could result in false alarms.

## 4. Proposed dos attack detection and mitigation framework

The mobile ad hoc networks (MANETs) are highly vulnerable to different kinds of security threats due to their dynamic nature of randomness, decentralization, and lack of central authority. The aim of this work is to propose an effective DoS attack detection and mitigation framework for MANETs using machine learning techniques such as SVM, Random Forest, Neural Network, and KNN. By generating synthetic traffic data to represent both normal and DoS attack scenarios, normalizing features, and splitting the data into training and testing sets, the framework enables the training and evaluation of various models. The best-performing model is then used to predict and visualize the traffic types in a simulated MANET environment, helping to identify attack nodes and measure key performance metrics like energy consumption, scalability, resource utilization, and network throughput. The description of attack detection and mitigation framework is given in figure 2 below:

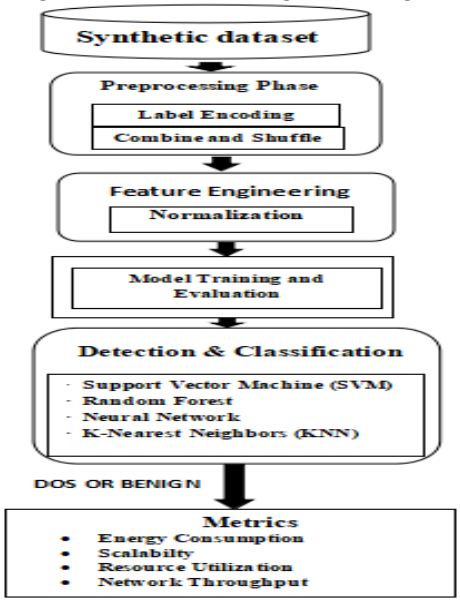


Fig. 2. Attack Detection and Mitigation Framework

This approach provides a systematic way to enhance security and resilience against DoS attacks in MANETs. The machine learning models such as SVM, Random Forest, Neural Network, and KNN are used to detect DoS attacks based on traffic characteristics and network behavior. The features, labels, and attributes are derived from the synthetic traffic data generated during the simulation. Given the predictive power and analytical capabilities of these models, they are well-suited for identifying and managing DoS attacks in Mobile Ad-hoc Networks (MANETs). The performance of the proposed detection and mitigation framework is illustrated by simulating various network conditions and evaluating key metrics such as energy consumption, scalability, and network throughput. The framework, utilizing the best-performing model, will be demonstrated through a simulated MANET environment to showcase its effectiveness in attack detection and mitigation.

### 4.1 Data generation

We create a synthetic dataset to simulate normal traffic and DoS attack traffic:

Normal Traffic Generation:

Let:

$X_{normal} = [x_1, x_2]$ be the matrix for the normal traffic

$X_1 \sim N(\mu_1 \sigma_1^2)$, where μ1=50 and σ1=15

$X_2 \sim N(\mu_2, \sigma_2^2)$, where μ1=10 and σ1=3

Each data point for normal traffic is sampled from the distributions:

$$X_{normal} = \begin{matrix} x_{11} & x_{12} \\ x_{21} & x_{22} \\ \dots & \dots \end{matrix}$$

Where $X_{i1} \sim N(50, 15^2)$, and $X_{i2} \sim N(10, 3^2)$

DoS Attack Traffic Generation:

Also, let:

. $X_{attack} = [y_1, y_2]$ be the feature matrix for DoS attack traffic

$y_1 \sim N(\mu_3, \sigma_3^2)$, where $\mu_3 = 50, \sigma_3 = 25$

$y_2 \sim N(\mu_4, \sigma_4^2)$, where $\mu_4 = 50, \sigma_4 = 2$

Each data point for attack traffic is sampled from these distributions

$$X_{attack} = \begin{matrix} y_{11} & y_{12} \\ y_{21} & y_{22} \\ \dots & \dots \end{matrix}$$

Where $Y_{i1} \sim N(150, 25^2)$, and $Y_{i2} \sim N(5, 5^2)$

Label Assignment:

Assign labels:

$$\text{Lebel} = \begin{cases} 0 & \text{normal} \\ 1 & \text{attack} \end{cases}$$

### 4.2 Model training

The objective is to train several machine learning models to classify network traffic as either normal or an attack.

Support Vector Machine (SVM):

SVM aims to find a hyperplane that best separates the two classes:

$$\text{minimum } \frac{1}{2}\|w\|2 \quad \text{subject to } y_i(w.x_i + b) \geq 1, \forall_i$$

Where:

w is the weight vector defining the hyperplane.

b is the bias term.

$y_i \in (-1,1)$ are the class labels.

$x_i$ are the feature vectors.

Random Forest Classifier

A Random Forest classifier is an ensemble of decision trees T1, T2,……,Tm. For each tree:

$$\text{Class} = \text{majority vote } (T_1(x), T_2(x), \ldots . T_m\ (x))$$

Where:

$T_i(x)$ is the prediction of the ith tree for input x

Neural Network (MLP Classifier)

The Neural Network model consists of an input layer, hidden layers, and an output layer:

$$\text{Output} = f(W2 \cdot (f(W1 \cdot X + b1)) + b2)$$

Where:

X is the input feature matrix.

W1,W2 are the weight matrices for the input-to-hidden and hidden-to-output layers.

bi, b2 are the bias vectors.

f is the activation function

K-Nearest Neighbors (KNN)

For KNN, the class of a new point x is determined by the majority class among its k-nearest neighbors:

$$\text{Class}(x) = \text{argmax}_c \sum_{i \in N_k(x)} \| (y_i = c)$$

where:

$N_k(x)$ is the set of the k-nearest neighbors to point x.

$\|$ is the indicator function that returns 1 if $y_i = c$, and 0 otherwise.

### 4.3 Proposed Algorithm for Dos Attack Detection and Mitigation in Manets

The proposed algorithm for Dos attack detection and mitigation are given below:

**Algorithm 1** DoS Attack Detection in MANET

**Input:** Number of samples *num_samples* = 2000
**Output:** Detection accuracy and performance metrics for various ML models
**Step 1: Generate Synthetic Dataset**
Set random seed for reproducibility
Generate normal traffic data:
Feature 1: Normal distribution with mean = 50, std = 15
Feature 2: Normal distribution with mean = 10, std = 3
Generate DoS attack traffic data:
Feature 1: Normal distribution with mean = 150, std = 25
Feature 2: Normal distribution with mean = 5, std = 2
Label normal traffic as 0 and DoS attack traffic as 1
Combine normal and attack traffic data
Shuffle the dataset to ensure randomness
**Step 2: Feature Engineering**
Normalize the features using *StandardScaler*
**Step 3: Split Dataset**
Split the dataset into training (70%) and testing (30%) sets
**Step 4: Train and Evaluate Models**
Initialize the following models:
- Support Vector Machine (SVM)
- Random Forest
- Neural Network
- k-Nearest Neighbors (KNN)
**for** each model **do**
Train the model on the training set
Predict labels on the testing set
Calculate accuracy, confusion matrix, and classification report
Store evaluation results
**end for**

**Algorithm 2** DoS Attack Mitigation in MANET

**Input:** Trained ML model (e.g., Neural Network), MANET network simulation
**Output:** Mitigation strategy performance in a simulated MANET
**Step 1: Visualize Network Traffic**
Simulate a MANET with nodes
Generate node positions using a layout algorithm
**for** each node **do**
Predict traffic type (normal or DoS attack) using the best-performing model (e.g., Neural Network)
Assign color based on prediction:
- Red for DoS attack traffic
- Blue for normal traffic
**end for**
Draw the network graph with nodes and edges
Display the network graph
**Step 2: Simulate and Analyze Performance Metrics**
Simulate performance metrics for each model:
- Energy Consumption (arbitrary units)
- Scalability (arbitrary units)
- Resource Utilization (arbitrary units)
- Network Throughput (Mbps)
Plot bar graphs for each performance metric

## 5. Experimental design

The main aim is to evaluate and compare the effectiveness of various machine learning models in detecting and mitigating DoS attacks in MANETs. The proposed DoS attack detection and mitigation model was implemented and validated using Python, along with Scikit-learn libraries, within the Google Colab environment. All evaluations were conducted on a Dell machine equipped with an Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz to 1.90 GHz. The framework involved generating synthetic datasets to simulate normal and DoS attack traffic, training various machine learning models (SVM, Random Forest, Neural Network, KNN), and

evaluating their performance. The best-performing model was used to predict traffic types in a simulated MANET environment, with performance metrics such as energy consumption, scalability, resource utilization, and network throughput being analyzed to validate the effectiveness of the detection and mitigation strategies.

### 5.1 Data collection and preprocessing

Data Preparation**:** Synthetic datasets are generated to represent normal traffic and DoS attack traffic. The data includes features that are crucial for detecting anomalies, such as traffic patterns and attributes. These datasets are labeled accordingly and combined to create a comprehensive dataset for model training. Feature Engineering: The features from the dataset are normalized using StandardScaler to ensure consistency and effectiveness in model training.

### 5.2 Model training and evaluation

Different machine learning models, including SVM, Random Forest, Neural Network, and KNN, are trained on the prepared dataset. Each model learns to distinguish between normal and DoS attack traffic based on the features provided. The performance of each model is then evaluated using accuracy, confusion matrix, and classification reports. Training machine learning models:

Training SVM

SVM Accuracy: 0.9908

Table 1: Confusion Matrix for SVM:

| | | Actual Class: Positive | Actual Class: Negative |
|---|---|---|---|
| Predicted Class | Positive | 601 | 1 |
| | Negative | 10 | 588 |

Training Random Forest

Random Forest Accuracy: 0.9917

Confusion Matrix for Random Forest:

| | | Actual Class: Positive | Actual Class: Negative |
|---|---|---|---|
| Predicted Class | Positive | 601 | 1 |
| | Negative | 9 | 589 |

Training Neural Network

Neural Network Accuracy: 0.9925

Confusion Matrix for Neural Network:

| | | Actual Class: Positive | Actual Class: Negative |
|---|---|---|---|
| Predicted Class | Positive | 601 | 1 |
| | Negative | 8 | 590 |

Training KNN

KNN Accuracy: 0.9900

Confusion Matrix for KNN:

| | | Actual Class: Positive | Actual Class: Negative |
|---|---|---|---|
| Predicted Class | Positive | 600 | 2 |
| | Negative | 10 | 588 |

### 5.3 Network simulation and visualization

A simulated MANET environment is set up where the best-performing model is used to predict the type of traffic (normal or attack) for each node. The network is visualized with nodes colored based on these predictions to illustrate the impact of the DoS attack and the effectiveness of the detection model as shown in the figure below:

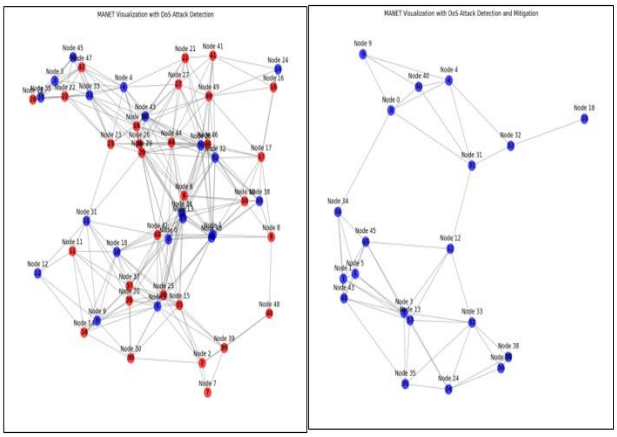

Fig. 3. MANET visualization with DoS Attack Detection and Mitigation Framework

## 6. Results and Analysis

### 6.1. Accuracy Comparison

Having an accuracy of 99.25%, Neural Network is the most accurate, followed by Random Forest (99.17%), SVM (99.08%), and KNN (99.00%). All four of the models are very effective at detecting and mitigating Denial of Service (DoS) assaults in a Mobile Ad-Hoc Network (MANET) environment, as seen by the little discrepancies in accuracy between them.

### 6.2 Classification Report Analysis

With 1.00 precision for both classifications (attack and benign traffic) across all models, there are very few false positives. For all models, the recall for class 0.0 (benign traffic) is 1.00, indicating that nearly all benign traffic is correctly identified. Recall is a bit lower for class 1.0 (attack traffic) for SVM and Random Forest, and 0.99 for Neural Network. The models demonstrate a consistent F1-score of 0.99, which is a measure of both precision and recall, indicating that their performance is balanced.

### 6.3 Confusion Matrix Analysis

All the four models have very similar confusion matrices, which show the following:

True Positives (TP) (correctly classified benign traffic) are around 600 out of 601 for all models. True

Negatives (TN) (correctly classified DoS attack traffic) are slightly varied but high in all models (588 for SVM, 589 for Random Forest, and 590 for Neural Network). False Positives (FP) (benign traffic incorrectly classified as attacks) are consistently 1 for almost all of the models except KNN which obtain a value of 2. False Negatives (FN) (attack traffic incorrectly classified as benign) are lowest for the Neural Network (8) and slightly higher for SVM and KNN (10) and also Random Forest (9).

### 6.4 Performance Metrics for Evaluation

The proposed framework simulates and plots performance metrics such as energy consumption, scalability, resource utilization, and network throughput. This helps to assess the overall impact of the DoS attack and the efficiency of the mitigation strategies employed.

Energy Consumption of the models. Figure 4 display the energy consumption of different machine learning models, The Neural Network model shows the highest energy consumption, followed by Random Forest and SVM, with KNN having the lowest. High energy consumption in Neural Networks can be due to complex computations required during the training and prediction processes. KNN's lower energy consumption makes it a more energy-efficient option, although it might sacrifice some detection accuracy.

#### 6.4.1 Scalability

Scalability is crucial for MANET environments where the number of nodes and traffic can vary significantly. Thus, Neural Networks and Random Forest are preferred for their scalability in handling large-scale network environments. The Neural Network and Random Forest models exhibit the best scalability, closely followed by SVM. KNN shows the lowest scalability, likely due to its distance-based classification approach, which can become computationally expensive with larger datasets.

#### 6.4.2 Resource Utilization

Higher resource utilization indicates that these models require more computational power, which could be a consideration when deploying in resource-constrained environments typical of MANETs. Random Forest and Neural Network models have the highest resource utilization, slightly above SVM, with KNN showing the lowest.

#### 6.4.3 Network Throughput

Higher throughput in the Neural Network model suggests it effectively handles larger volumes of network traffic, identifying and mitigating DoS attacks while maintaining network performance. The lower throughput observed in the KNN model indicates it might not be as effective in high-throughput scenarios, potentially leading to network congestion or slower attack detection. Neural Network demonstrates the highest network throughput, followed by Random Forest, SVM, and lastly KNN.

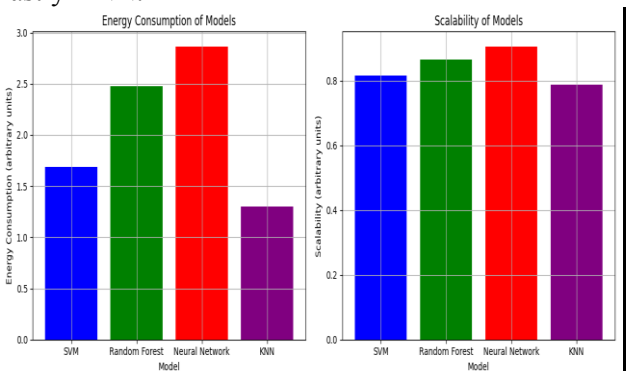


Fig. 4. Energy Consumption and Scalability of the Model

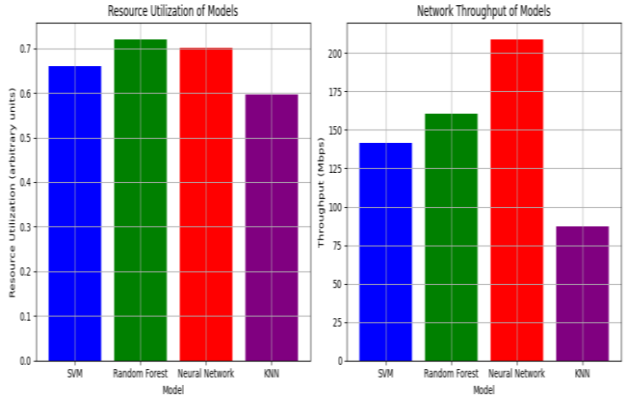


Fig. 5. Resource Utilization and Network Throughput of the Model

## 7. Discussion

Neural networks are the best choice in situations when high accuracy and the capacity to handle intricate patterns with superior recall and precision are required. Performance-critical applications can benefit from their use because they have the highest network throughput and energy consumption among them. An excellent substitute is Random Forest, which provides great accuracy with minimal false positives and negatives. It is a well-rounded option in most situations due to its excellent resource efficiency, good scalability, and modest energy consumption. SVM works well for basic tasks where managing complicated data is not as important as speed and simplicity. Its resource utilization, scalability, and energy consumption are all moderate, but its false negative rate is a little higher. KNN works well in simpler circumstances and with smaller datasets, it performs poorly in terms of network throughput, resource usage, and scalability. It performs well in contexts with limited resources and manageable data volumes.

The Neural Network model, while having higher energy consumption and resource utilization, offers

the best throughput and scalability. This suggests that Neural Networks are more suited for scenarios where performance and scalability are prioritized, even if it means using more energy and computational resources. Random Forest also shows a balanced performance with good scalability and resource utilization, making it a strong alternative for environments where energy efficiency is a secondary concern. SVM offers moderate performance across all metrics, making it an option when balanced performance is required. KNN is the most energy-efficient and uses the least resources but falls behind in scalability and throughput, making it less suitable for larger or high-traffic MANET scenarios. These insights help in selecting the appropriate machine learning model for DoS attack detection and mitigation based on the specific requirements of the MANET environment, balancing the trade-offs between energy consumption, scalability, resource utilization, and throughput.

## 7. Conclusion and Future Research Directions

The proposed framework for detecting and mitigating DoS attacks in Mobile Ad-hoc Networks (MANETs) leverages machine learning models like SVM, Random Forest, Neural Networks, and KNN to enhance network security. By generating synthetic datasets that simulate both normal and malicious traffic, the framework trains these models to distinguish between benign and attack traffic effectively. The performance evaluation reveals that Neural Networks provide the highest throughput and scalability, making them suitable for high-traffic environments, while models like KNN offer better energy efficiency, which is crucial in resource-constrained scenarios. the proposed framework can significantly contribute to the development of more secure and resilient MANETs, supporting critical applications that rely on reliable and protected network communication.

Future research directions should include exploring the use of advanced deep learning models such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. Additionally, adaptive mechanisms that adjust to changing attack patterns and network conditions could be developed, enhancing the system's ability to respond to threats in real time. Another significant area for future research is the development of hybrid detection models that combine multiple machine learning techniques to leverage their respective strengths. For instance, integrating SVM, Random Forest, Neural Network, and KNN into ensemble approaches could improve detection rates and reduce false positives. Extending the framework to detect a wider range of attacks would also make the system more comprehensive and robust against various types of security threats. Lastly, optimizing the energy efficiency of the detection models is crucial, especially in the context of MANETs where nodes often have limited power resources. Future work could focus on developing lightweight algorithms that reduce computational overhead while maintaining high detection accuracy. Testing the framework in real-world scenarios with actual network traffic data and resource-constrained environments, such as IoT-integrated MANETs, will provide valuable insights into its practical applicability.

*References:*

*[1] R. R. L. a. C. R. K. Reddy, "Node activity based trust and reputation estimation approach for secure and QoS," International Journal of Electrical & Computer Engineering (IJECE), no. 6, , vol. vol 9, pp. pp. 5340-5350, 2019.*

*[2] P. C. a. T. Ranganayaki, "A Study on Manet: Applications, Challenges and Issues," International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, no. Special Issue - 2020, 2020.*

*[3] R. A. A. a. R. A. Maha Abdelhaq, "The resistance of routing protocols against DDOS attack in MANET," International Journal of Electrical and Computer Engineering (IJECE), Vols. Vol. 10, No. 5, p. pp. 4844~4852, 2020.*

*[4] P. Nayak and B. Vathasavai, "Impact of random mobility models for reactive routing protocols over MANET," International Journal of Simulation--Systems, Science & Technology, , Vols. vol. 17,, pp. pp. 13.1-13. 9,.*

*[5] M. Y. N. Uparosiya, ""Survey on MANET: Routing protocols, advantages, problems and security,"," International Journal of Innovative Computer Science & Engineering,, vol. vol. 1, pp. no. 2, pp. 12-17.*

*[6] e. a. A. D. Basheer, "SIEM-based detection and mitigation of IoT-botnet DDoS attacks,," International Journal of Electrical &*

*Computer Engineering, , vol. vol. 10, pp. pp. 2182-2191,, 2020.*

*[7] I. S. H. K. J. E. a. D. G. Fatemeh Safari, "The Diverse Technology of MANETs: A Survey of Applications and Challenges," International Journal of Future Computer and Communication,, Vols. Vol. 12, No. 2, , p. 12, 2023.*

*[8] M. C. a. E. M. S. Er. Inakshi Garg, "DOS Attack Mitigation In MANET," International Journal of Computer Science Engineering (IJCSE), Vols. ISSN : 2319-7323, p. 05.*

*[9] .. M. I. O. S. O. Baraa T. Sharef, "A survey on position-based routing protocols for Flying Ad hoc Networks (FANETs)," Vehicular Communications, pp. Pages 29-56, 2017.*

*[10] A. M. F. A.-R. S. Saeed N. H., "MANET routing protocols taxonomy," in International Conference on Future Communication Networks,.*

*[11] N. Beijar, "Zone routing protocol (ZRP).," in Networking Laboratory, Helsinki University of Technology, 9, 1-12., Finland,, 2019.*

*[12] A. T. R. Y. a. D. A. K. Tawseef, "MANET Routing Protocols, Attacks and Mitigation Techniques: A Review," International Journal of Mechanical Engineering, Vols. ISSN: 0974-5823 Vol. 7 No. 2 , p. 11, 2022.*

*[13] T. S. H. E. S. M. A. K. Mohamad, "AN INTRUSION DETECTION MECHANISM FOR MANETS BASED ON DEEP LEARNING ARTIFICIAL NEURAL NETWORKS (ANNS)," International Journal of Computer Networks & Communications (IJCNC), vol. Vol.15, no. No.1, p. 15, 2023.*

*[14] R. K. K. V. R. G. Zalte S. S., "Mitigation of DDoS Attack in MANET," International Journal of Engineering and Advanced Technology (IJEAT),ISSN: 2249-8958 (Online), Vols. Volume-9 , no. Issue-6, , 2020.*

*[15] B. C. R. K. Jasmine, "DDoS Attack Detection and Prevention using Aodv Routing Mechanism and Ffbp Neural Network in a Manet",," International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Vols. Volume-8 , no. Issue-2,, pp. pp- 4136-4142, 2019.*

*[16] E. A. a. A. Shams, "A novel support vector machine based intrusion detection system for mobile ad hoc networks," Wireless Networks,, Vols. vol. 24, no. 5, , pp. pp. 1821-1829, 2020.*

*[17] A. J. H. a. A. L. Alsumayt et al, "Evaluation of Detection Method to Mitigate DoS Attacks in MANETs," in 1st International Conference on Computer Applications & InformationSecurity (ICCAIS),.*

*[18] E. H. A. S. H. a. L. K. Z. Abou, "Cochain-SC: An Intra- and Inter-Domain DDoS MitigationScheme Based on Blockchain Using SDN and Smart Contract," in In: Proceedings of the IEEE Access,, vol. 7, pp. 98893-98907, 2019.*

*[19] a. P. B. S. Payal N. Raj, "DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK INAODV BASED MANET," International Journal of Computer Science Issues,, Vols. Vol. 2,, pp. PP 54-59, 2019.*

*[20] C. R. K. Jasmine Batra, "DDoS Attack Detection and Prevention using Aodv Routing Mechanism and Ffbp Neural Networkin a Manet," International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878,, Vols. Volume-8, no. Issue-2,, pp. pp- 4136-4142 .*